Software Assurance Forum March 2009

Common Software Assurance Findings Schema Effort

Sean Barnum
Cigital Federal, Inc.
sbarnum@cigital.com

Today's Reality in Software Assurance Analysis

- Every SwA tool and service provider reports its findings in its own proprietary schematic format
  - Different information provided
  - Different terminology
  - Different structure
  - Different complexity

Need for a Common Schema

- Multi-perspective integration challenges
- Multi-tool integration challenges
- Multiple assessment vendor challenges
- Automated results analysis challenges
  - Assessment automation challenges
- Trending challenges

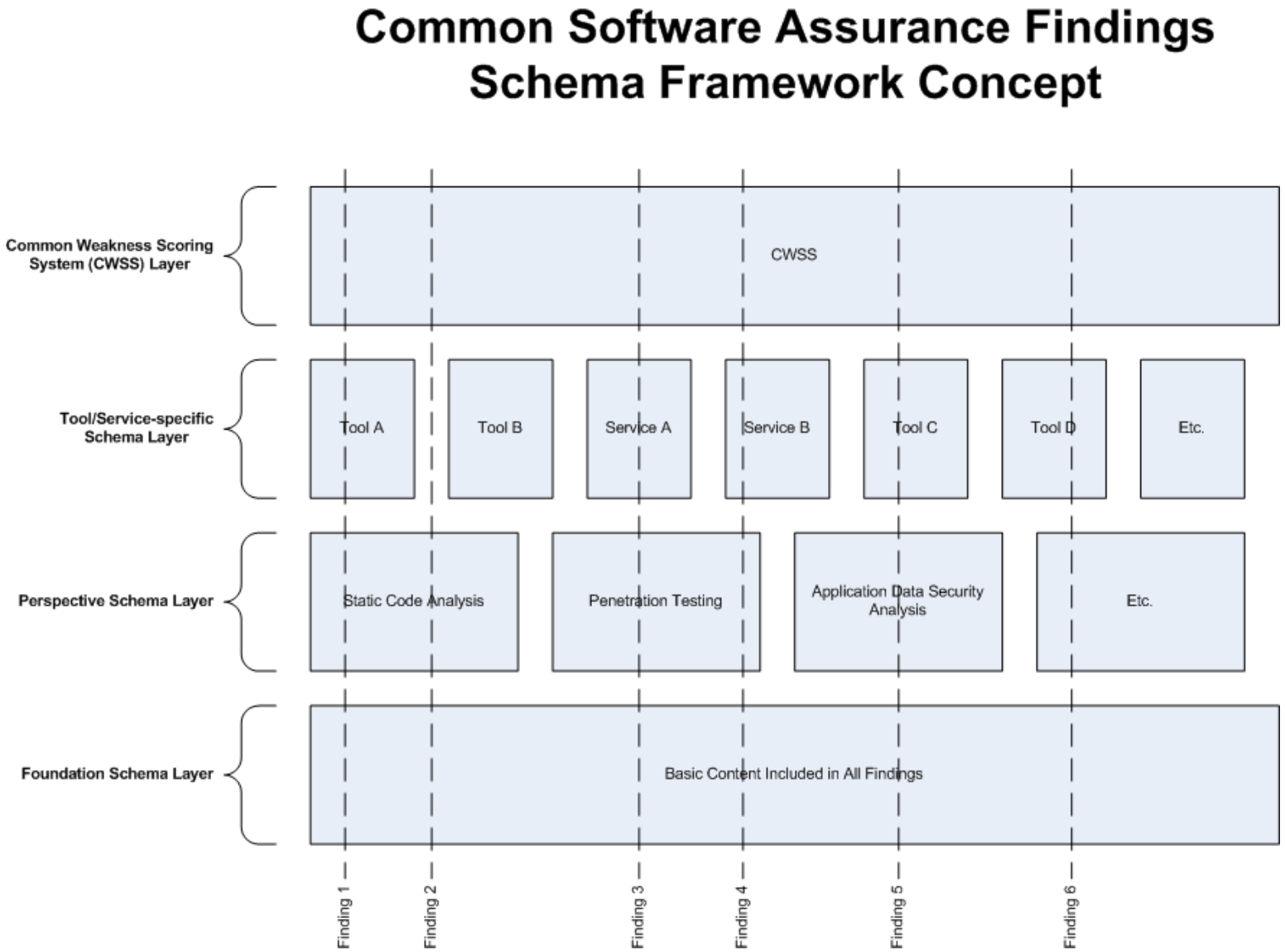
Value of a Common Schema

- Enable and encourage greater consistency in findings
  - Support trending
- Establish more structured tool results that are more useful to users
- Enable integration of results from multiple perspectives
- Enable integration of results from multiple tools and will enable automated processing of tool results

Flat Schema is Not Enough: A Framework is Needed

- Different perspectives, tools and techniques:
  - Look for different kinds of things
  - Look for things in different ways
  - Target different users
  - Differ in their capability to provide detail
  - Are of differing quality
- A universal flat schema would be much too large and unwieldy

What would a Framework Look Like?



Common Software Assurance Findings Schema Framework Effort

- History
  - Idea germinated years ago
  - Cigital feels pain of helping clients with multiple perspectives and multiple tools
  - Cigital feels pain of normalizing trending data
  - Was a common schema politically feasible with vendors?
    - Encouraging responses more and more common
- Need for action
  - Increasing popularity of multi-perspective and multi-tool approaches makes it imperative this problem be solved
- Current status
  - Initial sponsorship secured from government agency
  - Work began last week

Effort Approach

- Collaborative effort with Cigital providing primary technical leadership but with the involvement and contributions of an assortment of software assurance tool & service vendors willing to participate and other members of the software assurance community as appropriate
  - Capture state-of-the-practice in SwA findings schemas
  - Normalize and aggregate into common schema framework
  - Capture state-of-the-art and refine understanding
  - Review and revise schema framework with stakeholders
  - Deploy schema framework

Effort Planned Activities

- Create and adorn a tool taxonomy classifying and describing classes of tools and specific instances within classes
- Identify key representational tool instances
- Collect schema information from targeted tool instances
- Analyze aggregated schemas to capture state-of-the-practice
- Normalize and structure aggregated content into draft schema framework
- Research and evaluate state-of-the-art thinking in SwA findings communication and schema
- Revise and extend draft schema framework
- Distribute draft schema framework to targeted tool instance vendors for review
- Analyze review feedback and refine draft schema framework
- Distribute draft schema framework to SwA Community for review
- Analyze review feedback and refine draft schema framework
- Pilot draft schema framework
- Analyze pilot results and refine draft schema framework
- Deploy SwA findings schema framework

Opportunities for Involvement

- SwA tool & service vendors interested in volunteering schemas (can be done under NDA)
- SwA tool & service vendors interested in providing review feedback
- SwA tool & service vendors interested in piloting draft schema framework
- SwA community members interested in providing review feedback
- Any recommendations for state-of-the-art thinking
- Anyone willing to help evangelize